UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/640,839	08/16/2000	Mark Gregory McClanahan	RPS9-2000-0052US1	4229

45211	7590	03/10/2005

KELLY K. KORDZIK
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER
LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication..
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-81* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-81* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed 18 January 2005, with respect to claims 1-81 have been fully

considered and are persuasive. The previous claim rejections have been withdrawn, however,

grounds of rejection are re-introduced after further consideration of the He reference cited in the

Office Action dated 28 May 2004.

2.   Since the He reference was previously responded to by Applicant, the arguments dated 23

August 2004 will be addressed here.

3.   Applicant's arguments filed 23 August 2004 have been fully considered but they are not

persuasive. Applicant's argument that the He reference does not disclose an application

framework wherein said application framework logs on a user with a first level of access in said

underlying operating system is not persuasive because He discloses a system for single sign-on

to a plurality of network elements wherein users are allowed to log-on only once at a user station

and a Security Server will automatically log the user on to all the network elements that the user

is authorized to access (Col. 2, lines 25-32). The architecture and method for the Single Sign-on

system ("SSO") meets the limitation of providing an application framework. The SSO allowing

the user to log-on to the system meets the limitations of generating an application framework

sign-on screen, wherein said application framework logs on a user, and entering a logon input on

said generated application framework sign-on screen. The user accessing network elements that

the user is authorized to access and the database for user authorization and user privilege control

(Fig. 2) meet the limitation of user log-on with a first level of access in said underlying operating

system.

4.   Applicant's argument that the He reference does not disclose generating an application framework sign-on screen is not persuasive because the SSO allowing the user to log-on to the system meets the limitations of generating an application framework sign-on screen.

5.   Applicant's argument that the He reference does not disclose entering a logon input on said generated application framework sign-on screen is not persuasive because He discloses that the SSO receives user logon information (Col. 5, lines 7-14).

6.   Applicant's argument that the He reference does not disclose comparing said logon input with an application framework security database to determine level of access is not persuasive because when the user attempts to log-on the information entered by the user is checked against the information in the user profile of the central security database at the security server and assures that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-15).

7.   Applicant's argument that the He reference does not disclose selecting an indication of said first level of access is not persuasive because He discloses that the user attempts to log-on the information entered by the user is checked against the information in the user profile of the central security database at the security server and assures that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-15), which would also meet the limitation of wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on.

8.   Applicant's argument that the He reference does not disclose if said logon input is not entitled to a second level of access according to said application framework security database,

the said user is logged onto an application environment and said underlying operating system as

said first level of access is not persuasive because He discloses that the user privilege level

determines the access rights that the user has and what network elements the user can access

(Col. 5, lines 41-45). Unless the user is granted additional access rights (Col. 5, lines 45-48 &

Col. 8, lines 40-65), the user can only access the network elements designated to that user as

being authorized for their use, and attempted accesses of unauthorized network elements will be

rejected and logged (Col. 5, lines 49-58).

9.   Applicant's arguments that the He reference does not disclose generating an indication of

said second level of access and executing a switch user program to switch level of access to said

second level of access by selecting said indication of said second level of access is not persuasive

because He discloses that the SSO contains an indication digit for regular users and for super

users (Col. 10, line 58 – Col. 11, line 10).

10.   Applicant's arguments that the He reference does not disclose executing a switch user

program to switch said user to said second level of access is not persuasive because He discloses

that if a user log-on gives the user "super user" access rights then the user is provided with more

privileges to perform administrative functions in an network element (Col. 8, lines 51-54), which

further meets the limitation of if said underlying operating system security database verifies said

user with access to said second level of access, then said switch user program switches said user

to said second level of access.

11.   Applicant's argument that the He reference does not disclose said switch user program

switches said user to said second level of access by modifying an underlying operating system's

registry is not persuasive because He discloses that the user records, stored in registry (Col. 15,

lines 52-53), are modified to give the user more access rights (Col. 5, lines 41-48), which further meets the limitations of said switch user program switches said user to said second level of access by modifying an underlying operating system's registry, said switch user program switches said user to said second level of access by modifying an underlying operating system's registry.

12. Applicant's argument that the He reference does not disclose comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access is not persuasive because He discloses that if a user log-on gives the user "super user" access rights then the user is provided with more privileges to perform administrative functions in an network element (Col. 8, lines 51-54).

Claim Rejections - 35 USC § 112

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 9, 14, 21, 22, 27, 36, 41, 48, 49, 54, 63, 68, 75, 76, 81 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

15. Claims 9, 14, 21, 27, 36, 41, 48, 54, 63, 68, 75, 81 recite the limitation "logging off said user with first level of access, wherein said underlying operating system logs on said user with said second level of access" which renders the claim indefinite because it is unclear which level of access the user possesses.

16.   Claims 22, 49, 76, recite "comparing said logon input with an underlying operating

system security database, wherein if said underlying operating system security database does not

verify said user with access to said second level of access, then... requesting from said user a

logon identification and comparing said logon identification with said underlying operating

system security database" which renders the claim indefinite because process is circular in

nature. If the user is not authorized to a second level of access the application framework is just

going to keep requesting re-entry of the user information.

Claim Rejections - 35 USC § 102

17.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

18.   Claims 1-8, 10-13, 15-20, 22, 23, 28-35, 37-40, 42-47, 49, 50, 55-62, 64-67, 69-74 76,

77, are rejected under 35 U.S.C. 102(e) as being anticipated by He, U.S. Patent No. 5,944,824.

Referring to claims 1, 7, 28, 33, 55, 60, He discloses a system for single sign-on to a plurality of

network elements wherein users are allowed to log-on only once at a user station and a Security

Server will automatically log the user on to all the network elements that the user is authorized to

access (Col. 2, lines 25-32). The architecture and method for the Single Sign-on system ("SSO")

meets the limitation of providing an application framework. The SSO allowing the user to log-

on to the system meets the limitations of generating an application framework sign-on screen,

wherein said application framework logs on a user, and entering a logon input on said generated

application framework sign-on screen. The user accessing network elements that the user is

authorized to access and the database for user authorization and user privilege control (Fig. 2)

meet the limitation of user log-on with a first level of access in said underlying operating system.

When the user attempts to log-on the information entered by the user is checked against the

information in the user profile of the central security database at the security server and assures

that the user accesses the correct network elements based on the user privilege (Col. 5, lines 8-

15), which meets the limitation of comparing said logon input with an application framework

security database to determine level of access. The SSO system is incorporated with the security

server (Figs. 1 & 2), which meets the limitation of a processor, a memory unit operable for

storing a computer program operable for bypassing an initial sign-on screen of an underlying

operating system with a single sign capability, an input mechanism, an output mechanism, and a

bus system coupling the processor to the memory unit, input mechanism, and output mechanism.

Referring to claims 2, 3, 18, 29, 30, 45, 56, 57, 72, He discloses that the user attempts to

log-on the information entered by the user is checked against the information in the user profile

of the central security database at the security server and assures that the user accesses the

correct network elements based on the user privilege (Col. 5, lines 8-15), which meets the

limitations of selecting an indication of said first level of access, the user is logged onto said

underlying operating system and an application environment with said first level of access

thereby bypassing said initial sing-on screen of said underlying operating system with said single

sign-on.

Referring to claims 4, 10, 16, 24, 31, 37, 43, 51, 58, 64, 70, 78, He discloses that the user

privilege level determines the access rights that the user has and what network elements the user

can access (Col. 5, lines 41-45). Unless the user is granted additional access rights (Col. 5, lines

45-48 & Col. 8, lines 40-65), the user can only access the network elements designated to that

user as being authorized for their use, and attempted accesses of unauthorized network elements

will be rejected and logged (Col. 5, lines 49-58), which meets the limitation of if said logon input

is not entitled to a second level of access according to said application framework security

database, then said user is logged onto an application environment and said underlying operating

system as said first level of access.

Referring to claim 5, 23, 32, 50, 59, 77, He discloses that the user log-on information is a

user ID and password (Col. 2, lines 60-61).

Referring to claim 6, 17, 19, 22, 25, 34, 44, 46, 49, 52, 61, 71, 73, 76, 79, He discloses

that if a user log-on gives the user "super user" access rights then the user is provided with more

privileges to perform administrative functions in an network element (Col. 8, lines 51-54), which

meets the limitation of executing a switch user program to switch said user to said second level

of access.

Referring to claims 8, 13, 20, 26, 35, 40, 47, 53, 62, 67, 74, 80, He discloses that the user

records, stored in registry (Col. 15, lines 52-53), are modified to give the user more access rights

(Col. 5, lines 41-48), which meets the limitation of a user switching program switches said user

to said second level of access by modifying an underlying operating system's registry.

Referring claims 11, 12, 15, 38, 39, 42, 65, 66, 69, He discloses that the SSO contains an

indication digit for regular users and for super users (Col. 10, line 58 – Col. 11, line 10), which

meets the limitation of if said logon input is entitled to a second level of access according to said

application framework security database, then the method further comprises the step of

generating an indication of said second level of access, executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access.

Conclusion

19.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E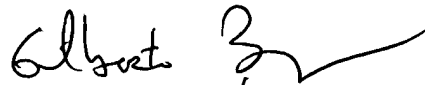 Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100